

# Triangular Canonical Forms for Lattice Rules of Prime-Power Order\*

J. N. Lyness and S. Joe

## Abstract

In this paper we develop a theory of  $t$ -cycle  $D - Z$  representations for  $s$ -dimensional lattice rules of prime-power order. Of particular interest are canonical forms that, by definition, have a  $D$ -matrix consisting of the nontrivial invariants. Among these is a family of *triangular* forms, which, besides being canonical, have the defining property that their  $Z$ -matrix is a column-permuted version of a unit upper-triangular matrix. Triangular forms may be obtained constructively by using sequences of elementary transformations based on elementary matrix algebra. Our main result is to define a unique canonical form for prime-power rules. This *ultratriangular* form is a triangular form, is easy to recognize, and may be derived in a straightforward manner.

## 1 Introduction

Let  $\Lambda_0$  be the *unit lattice*. This is the set of all  $s$ -dimensional points  $\mathbf{x} = (x_1, x_2, \dots, x_s)$ , all of whose components  $x_i$  are integers.

**Definition 1.1** *An  $s$ -dimensional lattice rule  $Q$  is an equal-weight quadrature rule on  $[0, 1)^s$ , which may be expressed in the form*

$$Qf = \frac{1}{d_1 d_2 \cdots d_t} \sum_{j_1=1}^{d_1} \sum_{j_2=1}^{d_2} \cdots \sum_{j_t=1}^{d_t} f \left( \left\{ \sum_{i=1}^t j_i \frac{\mathbf{z}_i}{d_i} \right\} \right), \quad (1.2)$$

where  $t$  and the  $d_i$  are positive integers,  $\mathbf{z}_i \in \Lambda_0$ , and  $\{\mathbf{x}\} \in [0, 1)^s$  denotes the vector whose components are the fractional parts of those of  $\mathbf{x}$ .

---

1991 *Mathematics Subject Classification*. Primary 65D30, 65D32.

*Key words and phrases*. Lattice rules, multidimensional quadrature.

\*This work was supported in part by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Computational and Technology Research, U.S. Department of Energy, under Contract W-31-109-Eng-38.

This form is known as a *t-cycle D – Z form* of an *s*-dimensional lattice rule [LK95]. It is abbreviated to

$$Q[t, D, Z, s],$$

where  $D$  denotes the  $t \times t$  diagonal integer matrix having positive diagonal elements  $d_i$  and  $Z$  denotes the  $t \times s$  integer matrix having rows  $\mathbf{z}_i$ .

The precursor of the lattice rule is the *number-theoretic* rule, introduced by Korobov [K59] and Hlawka [H62]. This is also defined by (1.2) above with  $t = 1$ . For an expository account of these rules we refer to Niederreiter [N78], [N88], and Hua and Wang [HW81]. A full history and detailed account of the current state of the theory of lattice rules appears in a recent monograph by Sloan and Joe [SJ94].

The  $D – Z$  form (1.2) has been used to derive many interesting results about lattice rules (see, for example, [SL89] or [SL90]). It suffers from two drawbacks. First, there are many different  $D – Z$  forms for the same rule. For example, it is easy to verify that the simple two-dimensional seven-point lattice rule

$$Qf = \frac{1}{7} \sum_{j=1}^7 f\left(\left\{\frac{j}{7}(1, 2)\right\}\right) \quad (1.3)$$

may be expressed as

$$Qf = \frac{1}{7} \sum_{j=1}^7 f\left(\left\{\frac{j}{7}(k, 2k)\right\}\right),$$

with  $k$  any integer relatively prime to 7. Other forms of the same rule include

$$Qf = \frac{1}{14} \sum_{j=1}^{14} f\left(\left\{\frac{j}{14}(2, 4)\right\}\right) \text{ and } Qf = \frac{1}{49} \sum_{j_2=1}^7 \sum_{j_1=1}^7 f\left(\left\{\frac{j_1}{7}(1, 2) + \frac{j_2}{7}(5, 3)\right\}\right). \quad (1.4)$$

All these are equivalent to (1.3). The second drawback to this form is that it may be *repetitive*. This is illustrated in the final two forms; each quadrature point occurs twice in the second form and seven times in the third form. Much of the theory is concerned with avoiding difficulties that arise because of this.

To return to the general  $D – Z$  form (1.2), we note that it specifies  $\det D = d_1 d_2 \cdots d_t$  abscissae, namely, the set

$$\mathcal{A}(Q) = \left\{ \left\{ \sum_{i=1}^t j_i \frac{\mathbf{z}_i}{d_i} \right\} : j_\ell \in [1, d_\ell], \ell \in [1, t] \right\}. \quad (1.5)$$

As we have just seen, the elements need not be distinct. The number of distinct abscissae required by  $Q$  is referred to as the order of  $Q$  and is written  $\nu(Q)$ . It is the number of *distinct* elements belonging to the set given in (1.5).

**Definition 1.6** *Let  $Q[t, D, Z, s]$  be a  $D – Z$  form of  $Q$ . It is termed nonrepetitive if*

$$\nu(Q) = \det D = d_1 d_2 \cdots d_t.$$

Forms (1.4) above are repetitive. It is simple to show that for all forms

$$\nu(Q) = \det D/k = d_1 d_2 \cdots d_t/k, \quad (1.7)$$

where  $k$  is a positive integer satisfying  $k \mid \det D$ . When  $k = 1$ , the form is nonrepetitive. Incidentally, when  $t > s$  and  $\nu(Q)$  is a power of some prime, an inequality stronger than (1.7) is valid. Under these circumstances  $\nu(Q)$  cannot exceed the product of the  $s$  largest elements  $d_i$  (see Theorem 3.10 below).

The proliferation of different  $D - Z$  forms for the same rule presents a challenge to find a special unique  $D - Z$  representation. However, except for the special case of projection-regular rules (see [SL90]), no unique  $D - Z$  form representation has appeared before. In [SL89] a general partial solution is given. For every rule  $Q$  one can find a canonical form  $Q[r, D, Z, s]$  in which  $r \leq s$ , the diagonal elements of  $D$  satisfy  $d_{i+1} \mid d_i$  and  $d_r > 1$ , and  $Z$  is of full rank. It turns out that for a given  $Q$  only one value of  $r$  and one matrix  $D$  satisfy these specifications;  $r$  is known as the rank and the elements  $d_1, \dots, d_r$  are the invariants of  $Q$ . However, many possibilities for  $Z$  remain.

In this paper we shall show that it is possible to obtain a *unique*  $D - Z$  representation for a *prime-power* rule, that is, a rule  $Q$  for which  $\nu(Q)$  is a positive power of some prime (greater than 1). In this unique *triangular* form,  $Z$  is a column-permuted unit upper-triangular matrix. The proofs are constructive so it is straightforward to develop an algorithm that produces this form for a prime-power rule.

Some further background material that applies to all rules is covered in the next section. The unique triangular form is developed in the remaining sections, which are devoted to prime-power rules.

## 2 Background Material

A vast number of different  $D - Z$  forms are available to describe the same lattice rule  $Q$ . However, these may be related by using a sequence of simple transformations to  $t$ ,  $D$ , and  $Z$  that leave the rule  $Q$  invariant. We list some of these below.

**Theorem 2.1** *The rule  $Q[t, D, Z, s]$  is unchanged if  $t$ ,  $D$ , and  $Z$  are modified by applying one of the following transformations, or a sequence of them.*

- (i) Replace  $\mathbf{z}_i$  by  $\ell \mathbf{z}_i$  for  $\ell$  an integer satisfying  $\gcd(\ell, d_i) = 1$ .
- (ii) Replace  $\mathbf{z}_i$  by  $\mathbf{z}_i + d_i \mathbf{x}$  for  $\mathbf{x} \in \Lambda_0$ .
- (iii) Replace  $\mathbf{z}_i$  by  $\mathbf{z}_i + (md_i/d_j)\mathbf{z}_j$  for  $j \neq i$ ,  $m$  an integer, and  $d_j \mid md_i$ .
- (iv) (Row interchange) Interchange  $d_i$  and  $d_j$  with a corresponding interchange of  $\mathbf{z}_i$  and  $\mathbf{z}_j$ .

- (v) (*Removal of overall common factor*) If  $\lambda$  is an integer for which  $d_i/\lambda$  is an integer and  $\mathbf{z}_i/\lambda \in \Lambda_0$ , replace  $d_i$  by  $d_i/\lambda$  and  $\mathbf{z}_i$  by  $\mathbf{z}_i/\lambda$ .
- (vi) (*Redundant row removal*) If  $d_t = 1$  or  $\mathbf{z}_t = \mathbf{0}$ , remove  $d_t$  from  $D$  and remove  $\mathbf{z}_t$  from  $Z$ . Then decrease the current value of  $t$  by 1.

Proofs or demonstrations of the validity of each of these transformations are very simple. The first three, given explicitly in [SL90], are the ones that retain  $t$  and  $D$  and alter rows of  $Z$  only. The remaining three (interchange of rows, elementary scaling, and redundant row removal) are trivial.

In view of the large number of  $D - Z$  forms available *ab initio* that describe the same lattice rule, the rest of this section is devoted to a few minor definitions that reduce the number of essentially trivial variants that we need to consider.

The reader will have noticed that in any  $D - Z$  form, one may arbitrarily reorder the rows  $Z$ , making a corresponding change in the order of the elements  $d_i$ . And, unless this is the only element of  $D$ , one may remove  $d_i$  and  $\mathbf{z}_i$  when  $d_i = 1$ . It is convenient to define the following.

**Definition 2.2**  *$D$  is sequential or a  $D - Z$  representation is sequential if*

$$d_1 \geq d_2 \geq \cdots \geq d_t > 1.$$

To “reduce” any  $D - Z$  representation to a sequential representation is, in general, a trivial task.

There are many ways of representing an individual point  $\mathbf{z}/d$ .

**Definition 2.3** *The vector  $\mathbf{z}/d$ , where  $\mathbf{z} \in \Lambda_0$  and  $d$  is a positive integer, is said to be in proper form if at least one of the components of  $\mathbf{z}$  is relatively prime with  $d$  and  $\mathbf{z}/d \in [0, 1)^s$ . (Colloquially,  $\mathbf{z}/d$  is in its lowest terms, and the point is in the integration region.)*

**Definition 2.4** *A  $t$ -cycle  $D - Z$  form is proper nontrivial if every element  $\mathbf{z}_i/d_i$ ,  $i \in [1, t]$ , is in proper form and if elements  $d_i = 1$  or  $\mathbf{z}_i = \mathbf{0}$  do not occur.*

Pedagogically, the final phrase is not necessary because there is no proper form for the origin  $\mathbf{0}$ . This point occurs in all lattice rules. The  $D - Z$  form includes this point, as may be seen in (1.2) by setting  $j_i = d_i$  for  $i \in [1, t]$ . The  $s$ -dimensional lattice rule

$$Qf = f(\mathbf{0})$$

is represented by (1.2) if, for all  $i \in [1, t]$ , either  $d_i = 1$  or  $\mathbf{z}_i = \mathbf{0}$ . We refer to this as the unit rule. This leads to an inconvenient but trivial exception.

**Theorem 2.5** *All lattice rules, with the single exception of the unit rule, may be expressed in a sequential, proper nontrivial  $D - Z$  form.*

The reader will readily confirm that any  $D - Z$  form may be reduced to this form by using the transformations of Theorem 2.1. Note that all but one of the three forms in (1.3) and (1.4) are proper nontrivial. This form, which can be obtained so easily, does have one interesting useful property.

**Theorem 2.6** *Let  $Q[t, D, Z, s]$  be a proper nontrivial form of  $Q$ . Then  $\nu(Q)$  has a factor  $d_i$  for all  $i \in [1, t]$ .*

**Proof.** A simple argument, based on the structure of (1.2) yields this almost self-evident result.  $\square$

**Corollary 2.7** *When  $Q$  is a prime-power rule, that is,  $\nu(Q) = p^\gamma$  for some prime  $p$  and positive integer  $\gamma$ , then the elements of  $D$  in any proper nontrivial form of  $Q$  have  $d_i = p^{\gamma_i}$ .*

### 3 A Triangular Form for Prime-Power Lattice Rules

In the remaining sections we restrict our attention to prime-power rules. The prime  $p$  is the same prime throughout these sections. This section is devoted to developing what we shall term (Definition 3.5 below) a triangular  $D - Z$  form. We shall see that such a triangular form is always available for prime-power rules. In Section 4 we shall show that it is a canonical form; and in Section 5 we shall specify a unique triangular form.

The following extension of the conventional unit upper triangular (uut) matrix plays a central role in our theory.

**Definition 3.1** *The  $t \times s$  matrix  $Z$  is termed column-permuted unit upper-triangular (cpuut) if and only if there exist distinct column indices  $\{\zeta_1, \zeta_2, \dots, \zeta_{\min(t,s)}\}$ , where  $\zeta_j \in [1, s]$ , and*

$$Z_{k, \zeta_m} = \begin{cases} 1, & \text{when } k = m, \\ 0, & \text{when } k > m, \end{cases} \quad m \in [1, \min(t, s)]. \quad (3.2)$$

When the column indices are  $\{1, 2, \dots, \min(t, s)\}$ , this is the conventional uut matrix. As an example we illustrate a  $7 \times 10$  cpuut matrix with column indices given by  $\{1, 2, 8, 6, 4, 5, 9\}$ . In this illustration,  $X$  and  $W$  represent integers. Note that there

are elements, denoted here by  $W$ , that are to the left (or west) of the pivot but need not be zero. Their significance will become apparent in Section 5.

$$\begin{bmatrix} 1 & X & X & X & X & X & X & X & X & X \\ 0 & 1 & X & X & X & X & X & X & X & X \\ 0 & 0 & W & W & W & W & W & 1 & X & X \\ 0 & 0 & W & W & W & 1 & X & 0 & X & X \\ 0 & 0 & W & 1 & X & 0 & X & 0 & X & X \\ 0 & 0 & W & 0 & 1 & 0 & X & 0 & X & X \\ 0 & 0 & W & 0 & 0 & 0 & W & 0 & 1 & X \end{bmatrix} \quad (3.3)$$

**Theorem 3.4** *Any  $D - Z$  form in which  $t \leq s$  and  $Z$  is cput is nonrepetitive.*

**Proof.** The abscissa set comprises all points of the form

$$\left\{ \sum_{i=1}^t j_i \frac{\mathbf{z}_i}{d_i} \right\}, \quad j_\ell \in [0, d_\ell), \quad \ell \in [1, t].$$

(Note that in these summations each parameter  $j_\ell$  could have been permitted to take any  $d_\ell$  consecutive integer values. Here it is more convenient to use the limits 0 and  $d_\ell - 1$  rather than the usual ones of 1 and  $d_\ell$ .) The condition that two distinct parameter choices  $j'_1, j'_2, \dots, j'_t$  and  $j''_1, j''_2, \dots, j''_t$  should describe the identical point implies that the point parameterized by their difference  $j'_1 - j''_1, j'_2 - j''_2, \dots, j'_t - j''_t$  is the origin. Thus, if this form is repetitive, there exist  $q_i \in [0, d_i)$ , not all zero, such that

$$\left\{ \sum_{i=1}^t q_i \frac{\mathbf{z}_i}{d_i} \right\} = \mathbf{0}.$$

Taking the  $\zeta_m$ -th component of this and applying (3.2) above yields

$$\left\{ \sum_{i=1}^{m-1} q_i \frac{Z_{i,\zeta_m}}{d_i} + \frac{q_m}{d_m} \right\} = 0.$$

Setting  $m = 1$  gives  $q_1 = 0$ ; when  $q_1 = q_2 = \dots = q_{j-1} = 0$ , setting  $m = j$  yields  $q_j = 0$ . It follows by induction that all coefficients  $q_i$  are zero, and so the form cannot be repetitive.  $\square$

**Definition 3.5** *A triangular form is a proper nontrivial form in which  $D$  is sequential and  $Z$  is cput.*

We recall from Definitions 2.2 and 2.4 that when  $D$  is sequential, all elements  $d_i$  exceed 1, and that in a proper nontrivial form, none of the  $\mathbf{z}_i$  are  $\mathbf{0}$ . Because  $Z$  is cput, it follows that in a triangular form the value of  $t$  cannot be greater than  $s$ . (If  $t$  were to exceed  $s$ , then all the elements of  $Z$  in rows  $s + 1, \dots, t$  would be zero and  $Z$  would then not be proper nontrivial.) A useful corollary of Theorem 3.4 is as follows.

**Corollary 3.6** *A triangular  $D - Z$  form is nonrepetitive.*

It was shown in Section 2 (see Theorem 2.5) that with one exception, any lattice rule could readily be expressed as described in the hypothesis of the next theorem.

**Theorem 3.7** *Let  $Q = Q[t, D, Z, s]$  be a prime-power rule expressed in proper non-trivial  $D - Z$  form with  $D$  sequential. Then it may be re-expressed in triangular form.*

Note that in view of Corollary 2.7, all elements of  $D$  are powers of the prime  $p$ . The proof of Theorem 3.7 is by induction. The key lemma follows.

**Lemma 3.8** *Let  $j$  be an integer belonging to  $[1, s]$ . Suppose the prime-power rule  $Q[t, D, Z, s]$  is a proper nontrivial  $D - Z$  form in which  $D$  is sequential and  $Z$  satisfies some of the cpunt conditions, namely, that there exist distinct column indices  $\{\zeta_1, \dots, \zeta_{j-1}\}$ , each belonging to  $[1, s]$  such that for  $m \in [1, j - 1]$*

$$Z_{m, \zeta_m} = 1, \quad Z_{k, \zeta_m} = 0, \quad k \in [m + 1, t]. \quad (3.9)$$

*Then there exists a  $D - Z$  form of the same rule, whose elements satisfy all of the above as written with  $j$  replaced by  $j' = j + 1$  and  $t$  replaced by  $t' \leq t$ .*

**Proof.** Let  $\mathbf{z}_j = (\theta_1, \theta_2, \dots, \theta_s)$ . Since  $\mathbf{z}_j/d_j$  is proper, at least one component of  $\mathbf{z}_j$ , say  $\theta_\ell$ , has no factor  $p$ . In view of Theorem 2.1(i), we may replace  $\mathbf{z}_j$  by  $\lambda \mathbf{z}_j \pmod{d_j}$ , where  $\lambda$  is such that  $\lambda \theta_\ell \equiv 1 \pmod{d_j}$ , and set column index  $\zeta_j = \ell$ . This leaves  $Z_{j, \zeta_j} = 1$ ; note that  $\mathbf{z}_j/d_j$  is still proper; elements of  $\mathbf{z}_j$  that were previously zero remain zero; and elements having a factor  $p$  retain this factor  $p$ .

In light of Theorem 2.1(iii), we may subtract any integer multiple of  $\mathbf{z}_j$  from  $\mathbf{z}_k$  when  $d_k \leq d_j$ ,  $j \neq k$ , that is, when  $k > j$ . Thus we may replace  $\mathbf{z}_k$  by  $\mathbf{z}_k - Z_{k, \ell} \mathbf{z}_j$ . It is easy to check that, after doing this,

$$Z_{k, \zeta_m} = 0, \quad k \in [m + 1, t], \quad m \in [1, j].$$

Finally, since we have altered  $\mathbf{z}_k$ ,  $k > j$ , some elements  $\mathbf{z}_k/d_k$  may no longer be proper. If necessary, we must apply the “housekeeping” transformations (ii), (v), and (vi) of Theorem 2.1 to reduce these to their lowest terms and to remove any row in which  $d_k = 1$  or  $\mathbf{z}_k = \mathbf{0}$ . Then we reorder these rows to make  $D$  sequential. The resulting form is as stated in the lemma.  $\square$

**Proof of Theorem 3.7** The proof follows by induction by noting that, when  $j = 1$ , the hypothesis of the induction step coincides with the hypothesis of Theorem 3.7. And when  $j = t'$ , the conclusion of the induction step coincides with the conclusion of the theorem; that is, the form is a triangular form.  $\square$

We close this section with a somewhat unsophisticated result, which is convenient later in defining a canonical form and placing bounds on invariants.

**Theorem 3.10** *Let  $Q[\tilde{t}, \tilde{D}, \tilde{Z}, s]$  be any  $D - Z$  representation of a prime-power rule  $Q$  in which  $\tilde{d}_1 \geq \tilde{d}_2 \geq \dots \geq \tilde{d}_t \geq 1$  and  $Q[t, D, Z, s]$  be a triangular form. Then  $d_i \leq \tilde{d}_i$  for  $i \in [1, t]$ , and*

$$\nu(Q) \leq \tilde{d}_1 \tilde{d}_2 \cdots \tilde{d}_T, \quad T = \min(\tilde{t}, s). \quad (3.11)$$

Note that the nonunit elements of  $\tilde{D}$  are sequential, but in addition  $\tilde{d}_i = 1$  and  $\tilde{\mathbf{z}}_i = \mathbf{0}$  may occur.

**Proof.** The proof is straightforward. Following Theorems 2.5 and 3.7, the first form may be reduced to triangular form using only the elementary transformations of Theorem 2.1. Each transformation leaves all diagonal elements unchanged, reduces one of them, removes one of them, or alters their order. However, if members of an ordered sequence are individually changed, but not increased, and then the sequence is put in order again, the value of the new  $i$ -th member does not exceed the value of the original  $i$ -th member. (This simple result is a specialization of Lemma 2 of [N73].) This leads directly to  $d_i \leq \tilde{d}_i$  for  $i \in [1, t]$ , and these inequalities applied to (1.7) yield (3.11).  $\square$

## 4 Canonical $D - Z$ Forms for Prime-Power Rules

In [SL89] the celebrated Kronecker group representation theory was applied to the group formed from the abscissa set of a rule  $Q$  to establish the following:

*Each lattice rule may be expressed in a nonrepetitive  $t$ -cycle  $D - Z$  form in which  $d_{i+1} \mid d_i$ ,  $i \in [1, t-1]$  and  $d_t > 1$ . Moreover, in such a representation, the values of  $t$  and of the  $d_i$  are unique to the rule  $Q$  and are termed the rank of  $Q$  and the invariants of  $Q$ . Such a form is termed a canonical form.*

The above was established in [SL89] for all lattice rules. In the context of prime-power rules, clearly any triangular form as defined in the preceding section satisfies these conditions to be a canonical form.

**Theorem 4.1** *Any triangular form  $Q[t, D, Z, s]$  of a prime-power lattice rule  $Q$  is a canonical form, that is,  $t$  is the rank of  $Q$  and the  $d_i$ ,  $i \in [1, t]$ , are the invariants.*

The reader who is already familiar with this theory may omit the first part of this section.

A nonabstract interpretation of an invariant as the order of some subgroup has been exploited by Lyness [L93]. To make this paper self-contained, we wish to establish



Theorem 4.1 without recourse to group theory. To this end we need to construct an independent *definition* of the *invariants* of an  $s$ -dimensional rule  $Q$ .

To do this, we first introduce the projections of an  $s$ -dimensional lattice rule. A  $w$ -dimensional projection of a lattice rule is obtained by removing the same set of  $s - w$  components from each abscissa. There are many  $w$ -dimensional projections of  $Q$ , depending on which set of components is removed, or equivalently which set is retained. We denote by  $Q^{\{i_1, i_2, \dots, i_w\}^s}$  the  $w$ -dimensional rule obtained from  $Q$  by *retaining* only the specified components. Here  $i_1, \dots, i_w$  are  $w$  distinct integers lying in  $[1, s]$ . It is trivial to show that any such projection of a lattice rule is another lattice rule. Moreover, we have the following readily verified result.

**Lemma 4.2** *The  $w$ -dimensional projection  $Q^{\{i_1, i_2, \dots, i_w\}^s}$  of a rule  $Q$  having representation  $Q[t, D, Z, s]$  has representation  $Q[t, D, \overline{Z}, w]$ , where  $\overline{Z}$  is obtained from  $Z$  by retaining only columns  $i_1, i_2, \dots, i_w$ .*

**Definition 4.3** *The invariants of a prime-power lattice rule  $Q$  are defined as*

$$n_1 = \sigma^1(Q), \quad n_w = \sigma^w(Q) / \sigma^{w-1}(Q), \quad w \in [2, t],$$

where

$$\sigma^w(Q) = \max_{i_1, \dots, i_w \in [1, s]} \nu \left( Q^{\{i_1, i_2, \dots, i_w\}^s} \right).$$

Each of the distinct  $w$ -dimensional projections of the  $s$ -dimensional rule  $Q$  has its own order, some integer between 1 and  $\nu(Q)$ . We have defined entities  $\sigma^w(Q)$  as the maximum of these orders, and the invariants  $n_i$  as the ratio of successive values of  $\sigma^w(Q)$ .

It is clear that the invariants  $n_i(Q)$  defined above are uniquely defined in terms of  $Q$ . They are independent of any  $D - Z$  representation that we might employ. This is all that is needed *pro tempore*. Later, their more familiar properties will appear.

**Lemma 4.4** *Let  $Q[t, D, Z, s]$  be a triangular form of a prime-power lattice rule  $Q$ . For  $w \in [1, t]$ , let  $Q^{\{i_1, i_2, \dots, i_w\}^s}$  be one of the  $w$ -dimensional projections of  $Q$ . Then*

$$\nu \left( Q^{\{i_1, i_2, \dots, i_w\}^s} \right) \leq d_1 d_2 \cdots d_w, \quad (4.5)$$

and equality prevails for at least one  $w$ -dimensional projection.

**Proof.** Lemma 4.2 shows that  $Q^{\{i_1, i_2, \dots, i_w\}^s} = Q[t, D, \overline{Z}, w]$ , where  $\overline{Z}$  is obtained from  $Z$  by retaining columns  $i_1, \dots, i_w$ . A direct application of Theorem 3.10 yields the inequality (4.5).

To show that we can obtain equality, let  $\{\zeta_1, \dots, \zeta_t\}$  be the column indices of the triangular form. If we take  $i_k = \zeta_k$ ,  $k \in [1, w]$ , the second part of (3.2) shows that rows  $w + 1, \dots, t$  of  $\overline{Z}$  contain only zeros. Retaining only the first  $w$  rows of  $\overline{Z}$ , one may verify that the resulting  $w$ -cycle  $D - Z$  form is triangular. It then follows from Corollary 3.6 that  $\nu \left( Q^{\{\zeta_1, \zeta_2, \dots, \zeta_w\}^s} \right) = d_1 d_2 \cdots d_w$ .  $\square$

This lemma shows that  $\sigma^w(Q)$  in Definition 4.3 coincides with  $d_1 d_2 \cdots d_w$  obtained from *any* triangular form of  $Q$ . It follows that  $n_i$  in this definition coincides with  $d_i$ , so establishing Theorem 4.1. The key point here is that the  $D$ -matrix in a triangular form is unique to  $Q$ . That is, a different reduction of a different representation of  $Q$  cannot lead to a different sequential  $D$ -matrix. This justifies our use of the term invariant without any recourse to the underlying group theory required in [SL89]. We now restate Theorem 3.10 in a trivially modified form.

**Theorem 4.6** *Let  $Q$  be a prime-power rule, having rank  $r$  and invariants  $n_1, n_2, \dots, n_r$ . Let  $Q[t, D, Z, s]$  be any  $D - Z$  form representing  $Q$ . Then*

$$n_i \leq \delta_i, \quad i \in [1, r],$$

*where  $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_r$  are the  $r$  largest elements of  $D$ .*

For a prime-power rule we have now defined a canonical form as any form  $Q[r, D, Z, s]$  which represents  $Q$  and in which  $r$  is the rank and  $D$  contains the invariants in order. We have demonstrated one canonical form, the triangular form of the preceding section. The rest of this section is concerned with the conditions that must be satisfied by  $Z$  for  $Q[r, D, Z, s]$  to be a canonical form.

**Definition 4.7** *When  $t \leq s$ , a  $t \times s$  matrix  $Z$  is rank-deficient modulo  $p$  if and only if there exist integers  $\lambda_i, i \in [1, t]$ , not all zero (modulo  $p$ ) such that*

$$\sum_{i=1}^t \lambda_i \mathbf{z}_i = \mathbf{0} \pmod{p}. \quad (4.8)$$

**Corollary 4.9** *When  $t \leq s$ , a  $t \times s$  matrix  $Z$  is rank-deficient modulo  $p$  if for some  $\mathbf{z}_i$ , all elements have a factor  $p$ , that is,  $\mathbf{z}_i \in p\Lambda_0$ .*

These are standard definitions adjusted in an obvious way to a special situation.

**Theorem 4.10** *A necessary and sufficient condition that  $Q[t, D, Z, s]$  should be a canonical form of a prime-power rule  $Q$  is that  $D$  is sequential and  $Z$  is full rank modulo  $p$ .*

**Proof.** Examination of Theorems 2.5 and 3.7, which justify the reduction of any prime-power rule to triangular form, reveals that the first four operations, (i)–(iv), of Theorem 2.1 do not alter  $\det D$ . In fact, they do not alter any individual  $d_i$ , but (iv) alters their order. Thus, if  $D$  is sequential, only two transformations of Theorem 2.1 alter the elements  $d_i$ ; these are (v) and (vi) (in the case  $\mathbf{z}_i = \mathbf{0}$ ). However, these can be applied only if either some  $\mathbf{z}_i$  and  $d_i$  have an overall factor (which must be a multiple of  $p$ ), or if  $\mathbf{z}_i = \mathbf{0}$ . In either case, in light of Corollary 4.9,  $Z$  is rank-deficient modulo  $p$ . Thus, in the process of reduction from a general  $D - Z$  form to

a triangular form, if one encounters a situation in which  $D$  is sequential and  $Z$  is of full rank modulo  $p$ , the rest of the reduction does not alter  $D$ . This establishes that the condition is sufficient.

On the other hand, if  $Z$  is not of full rank, a relation of form (4.8) above exists. This may be expressed in the form

$$\mathbf{z}_k - \sum_{i=1}^{k-1} \mu_i \mathbf{z}_i = \mathbf{0} \pmod{p},$$

where  $k$  is the largest index  $j$  for which  $\lambda_j \neq 0 \pmod{p}$ . Then successive use of transformation (iii) of Theorem 2.1 leads to  $\mathbf{z}_k = \mathbf{0} \pmod{p}$ . Since  $D$  is sequential, applying Theorem 2.1(v) or (vi) reduces  $t$  and reduces or removes some value of  $d_i$ . Thus  $t$  is not the rank, and the form is not a canonical form.  $\square$

We conclude this section with the following result.

**Theorem 4.11** *A necessary and sufficient condition for a  $D - Z$  form of a prime-power rule to be canonical is that it be nonrepetitive with sequential  $D$ .*

**Proof.** The proof follows from the circumstances that all canonical forms have the same matrix  $D$ ; and for one form (Theorem 3.4)  $\nu(Q) = \det D$ , the condition for the form to be nonrepetitive. On the other hand, for a repetitive form  $\nu(Q) < \det D$  invalidating the possibility that  $D$  contains only the invariants.  $\square$

## 5 Prime-Power Rules: A Unique Canonical Form

We look for a unique but recognizable canonical form for prime-power rules. For example, the triangular form is readily recognizable. To check that  $Z$  is cput and that  $D$  is sequential is the work of a moment. Up to now we have shown that  $D$  is unique. But there are still many possibilities, all cput, for  $Z$ . To obtain a different matrix  $Z$ , we might have chosen a different  $\zeta_j$  at the  $j$ -th stage of the reduction of Lemma 3.8. When  $d_k \geq d_j$ , we may subtract any multiple of  $(d_k/d_j)\mathbf{z}_j$  from  $\mathbf{z}_k$  without altering the rule. And when  $d_j = d_{j+1}$ , we may simply interchange  $\mathbf{z}_j$  and  $\mathbf{z}_{j+1}$ . In this section we proceed to place various additional conditions on  $Z$  with a view to making it unique. (Some of these may appear to be arbitrary.)

We deal first with the possibility of altering  $\mathbf{z}_k$  by adding or subtracting a multiple of  $\mathbf{z}_j$ . When  $k > j$ , this will destroy the cput property of  $Z$ . But, when  $k < j$ , one may apply transformation (iii) of Theorem 2.1 to replace  $\mathbf{z}_k$  by  $\mathbf{z}_k - \lambda(d_k/d_j)\mathbf{z}_j$  for any integer  $\lambda$ . Since  $\mathbf{z}_j$  has zeros in positions  $\zeta_1, \zeta_2, \dots, \zeta_{j-1}$ , this leaves the corresponding components of  $\mathbf{z}_k$  unaltered. Because  $Z_{j,\zeta_j} = 1$ , we may compel the values of  $Z_{k,\zeta_j}$  to lie in the interval  $[0, d_k/d_j)$  simply by setting  $\lambda$  to be the integer part of  $(d_j/d_k)Z_{k,\zeta_j}$ . Thus, in addition to (3.2), we now impose the restriction

$$Z_{k,\zeta_m} \in [0, d_k/d_m), \quad k \in [1, m-1]. \quad (5.1)$$

We have made this part of our specification (Definition 5.6 below) of an *ultratriangular form*, which will be unique. We may think of restriction (5.1) being applied separately after the triangular form of Theorem 3.7 has been obtained. However, it may be inserted into the algorithm implicit in the proof of Lemma 3.8. This induction step lemma then requires (5.1) for  $m \in [1, j-1]$  in addition to (3.9). This may be combined with the second part of (3.2) to yield

$$Z_{k, \zeta_m} \in [0, d_k/d_m), \quad k \neq m. \quad (5.2)$$

A consequence of imposing (5.1) is that when  $d_k = d_j$ , we find

$$Z_{k, \zeta_j} = Z_{j, \zeta_k} = 0. \quad (5.3)$$

One of these follows from the *cpuut* nature of  $Z$  (the first if  $k > j$ ). The other follows because the only integer element of  $[0, 1)$  is 0.

We now impose a second condition. This restricts the choice of indices  $\{\zeta_1, \zeta_2, \dots, \zeta_t\}$ . We recall that in the proof of Lemma 3.8,  $\zeta_j$  is chosen to be *any* value  $\ell$  for which the  $\ell$ -th component of  $\mathbf{z}_j$  has no factor  $p$ . We now remove this choice.  $\zeta_j$  is to be the smallest value of  $\ell$  for which the  $\ell$ -th component of  $\mathbf{z}_j$  has no factor  $p$ . Thus we choose the indices in a deterministic manner. This restriction is equivalent to

$$Z_{m,k}/p \text{ is an integer for } k \in [1, \zeta_m - 1]. \quad (5.4)$$

Note that this does not clash with the condition that  $m-1$  of these integers (namely, the ones in positions  $\zeta_1, \zeta_2, \dots, \zeta_{m-1}$ ) are zero as a result of  $Z$  being *cpuut*. This is illustrated in the  $Z$ -matrix (3.3) above. The elements denoted by  $W$  are those that have a factor  $p$ . One desirable feature of this restriction is that it goes nearly all the way to ensuring, that if a unit upper triangular  $Z$  is possible, it will be the unique form. Indeed, if all the  $d_i$  are distinct, this is already the case. It still appears that when  $d_k = d_{k+1}$ , one may find  $\zeta_{k+1} < \zeta_k$ . However, in view of (5.3) above, these rows of  $Z$  may be interchanged without violating earlier restrictions. Our final restriction is

$$d_k = d_{k+1} \Rightarrow \zeta_k < \zeta_{k+1}. \quad (5.5)$$

We conclude this section with a definition that embraces restrictions (5.1), (5.4), and (5.5) and with the major theorem of this section.

**Definition 5.6** *An ultratriangular  $D-Z$  form for a prime-power rule is one in which*

- (i)  $D$  is sequential,
- (ii)  $\mathbf{z}_i/d_i$  is proper,
- (iii)  $Z$  is *cpuut* with column indices  $\{\zeta_1, \zeta_2, \dots, \zeta_t\}$ ,
- (iv)  $Z_{m,k}/p$  is an integer for  $k \in [1, \zeta_m - 1]$ ,

- (v) if  $d_m = d_{m+1}$ , then  $\zeta_m < \zeta_{m+1}$ , and
- (vi)  $Z_{k,\zeta_m} \in [0, d_k/d_m)$ ,  $k \neq m$ .

Clearly (i), (ii), and (iii) simply assert that this is a triangular form. The conditions of (vi) for which  $k > m$  are already included in (iii). It will appear later that (iv) and (v) may be replaced by the condition on  $\{\zeta_1, \zeta_2, \dots, \zeta_t\}$  of Theorem 5.10 below. The rest of this section is devoted to proving the following:

**Theorem 5.7** *All prime-power rules  $Q$  have a unique ultratriangular  $D - Z$  form.*

We know already that  $t$  (the rank) and  $D$  (containing the invariants) are unique. To prove this theorem, we then need to show that  $Z$  is unique. In general, different triangular forms of the same rule may be based on different column indices. We now show that the column indices  $\{\zeta_1, \zeta_2, \dots, \zeta_t\}$  in an ultratriangular form are unique. It turns out that the  $t$ -tuple  $\{\zeta_1, \zeta_2, \dots, \zeta_t\}$  is the smallest of the various possibilities in the sense of the following standard lexicographic ordering.

**Definition 5.8** *Let  $\{\zeta_1, \zeta_2, \dots, \zeta_t\}$  and  $\{\zeta'_1, \zeta'_2, \dots, \zeta'_t\}$  both be  $t$ -tuples containing a permutation of a subset of the integers  $1, 2, \dots, s$ . This standard ordering is defined by*

$$\{\zeta_1, \zeta_2, \dots, \zeta_t\} < \{\zeta'_1, \zeta'_2, \dots, \zeta'_t\}$$

*when  $\exists \ell$  such that  $\zeta_k = \zeta'_k$  for  $k \in [1, \ell - 1]$  and  $\zeta_\ell < \zeta'_\ell$ .*

According to this ordering the “smallest”  $t$ -tuple possible is  $\{1, 2, \dots, t\}$ , while the “largest” one possible is  $\{s, s - 1, \dots, s - t + 1\}$ . If  $s \leq 9$ , the ordering coincides with the natural ordering of the  $s$ -digit integers (base 10). For example, with  $s = 9$  we have  $\{6, 4, 3\} < \{7, 1, 2\}$  simply because  $643 < 712$ .

**Definition 5.9** *A triangular  $D - Z$  form is termed to have a minimal  $t$ -tuple of column indices if there is no other triangular  $D - Z$  form of the same rule  $Q$  with a smaller  $t$ -tuple (in the sense of Definition 5.8).*

**Theorem 5.10** *For a prime-power lattice rule, a triangular  $D - Z$  form that satisfies items (i) through (v) of Definition 5.6 has a minimal  $t$ -tuple of column indices.*

**Proof.** To establish this result, we shall show first that for  $k < \zeta_\ell$  the  $k$ -th component of each abscissa of  $Q$  that has zeros in positions  $\zeta_1, \dots, \zeta_{\ell-1}$  is of the form  $\lambda p/d_\ell$  for some integer  $\lambda$ . To prove this latter result, we let

$$\mathbf{c} = \left\{ \sum_{i=1}^t j_i \frac{\mathbf{z}_i}{d_i} \right\}, \quad j_i \in [0, d_i),$$

be such an abscissa. Since  $\mathbf{c}$  has zeros in positions  $\zeta_1, \dots, \zeta_{\ell-1}$ , an argument similar to that used in the proof of Theorem 3.4 shows that  $j_i = 0$  for  $i \in [1, \ell - 1]$ .

Suppose  $d_\ell = d_{\ell+1} = \dots = d_{\ell+m} > d_{\ell+m+1}$ . Then application of item (v) of Definition 5.6 gives  $\zeta_\ell < \zeta_{\ell+1} < \dots < \zeta_{\ell+m}$ . Since we are treating  $c_k$  with  $k < \zeta_\ell$ , it follows that  $k < \zeta_i$  for all  $i \in [\ell, \ell + m]$ . Thus  $m + 1$  applications of item (iv) of Definition 5.6 reveal that  $Z_{i,k}/p$  is an integer for  $i \in [\ell, \ell + m]$ ; hence, the contribution to  $c_k$  from these  $m + 1$  terms is a multiple of  $p/d_\ell$ .

Finally for  $i \geq \ell + m + 1$ , we have  $d_i < d_\ell$  so that  $d_i = d_\ell/(\mu p)$ , for some  $\mu \geq 1$ . It then follows that each contribution to the abscissa  $\mathbf{c}$  has a  $k$ -th component that is a multiple of  $p/d_\ell$  (including possibly a zero multiple), and so  $\mathbf{c}$  has a  $k$ -th component of the form  $\lambda p/d_\ell$ .

To prove the desired result, let us suppose there was a smaller  $t$ -tuple, say  $\{\zeta'_1, \zeta'_2, \dots, \zeta'_t\}$ . Let  $\ell$  be the first index for which  $\zeta'_\ell < \zeta_\ell$ . Then we see that  $Q$  has an abscissa  $\mathbf{c}'$  that has a component  $1/d_\ell$  in position  $\zeta'_\ell$  and zeros in positions  $\zeta_1, \dots, \zeta_{\ell-1}$ . However, since  $\zeta'_\ell < \zeta_\ell$  and  $\mathbf{c}'$  has zeros in positions  $\zeta_1, \dots, \zeta_{\ell-1}$ , we have already shown above that the  $\zeta'_\ell$ -th component of  $\mathbf{c}'$  is of the form  $\lambda p/d_\ell$ . This is a contradiction. Thus there cannot be an index  $t$ -tuple smaller than the  $\{\zeta_1, \zeta_2, \dots, \zeta_t\}$   $t$ -tuple for the  $D - Z$  form satisfying items (i) through (v) of Definition 5.6.  $\square$

This is a great help. Given any rule, the invariants and the rank are fixed. It goes without saying that of all possible triangular forms, there must be one having a minimal  $t$ -tuple of column indices. And, of possibly many choices of  $Z$ , we have shown that our choice of ultratriangular form is one that employs such a minimal  $t$ -tuple.

**Lemma 5.11** *A triangular form in which the  $t$ -tuple of column indices is minimal and in which condition (vi) of Definition 5.6 is satisfied is unique to the prime-power rule  $Q$ .*

**Proof.** As has already been pointed out, we need only prove that  $Z$  is unique. We first use induction to prove that columns  $\zeta_1, \dots, \zeta_t$  of  $Z$  are unique. Suppose  $Z$  and  $W$  are two alternative forms of a  $Z$ -matrix having all the properties of Definition 5.6. Since both  $\mathbf{z}_k/d_k$  and  $\mathbf{w}_k/d_k$  are abscissae of  $Q$ , we define

$$\mathbf{c}_k = \frac{\mathbf{z}_k - \mathbf{w}_k}{d_k},$$

and this is also a lattice element. As such, it may be expressed in the form

$$\mathbf{c}_k = \sum_{i=1}^t j_{k,i} \frac{\mathbf{z}_i}{d_i}. \quad (5.12)$$

Theorem 5.10 shows that both  $Z$  and  $W$  have the same indices  $\zeta_1, \dots, \zeta_t$ . Also, since both  $Z$  and  $W$  are cpuat, then they have the same  $\zeta_1$ -th column (all elements being zero except for the first element which is 1).

Let us suppose columns  $\zeta_1, \dots, \zeta_{m-1}$  of  $Z$  coincide with the corresponding column of  $W$ , but that for some  $k$ ,  $Z_{k,\zeta_m} \neq W_{k,\zeta_m}$ . (Note that such a value of  $k$  must be less than  $m$ .) Taking components  $\zeta_1, \zeta_2, \dots, \zeta_{m-1}$  of (5.12) in turn, we find successively  $j_{k,1} = j_{k,2} = \dots = j_{k,m-1} = 0$ . Specializing to component  $\zeta_m$  gives

$$C_{k,\zeta_m} = \frac{Z_{k,\zeta_m} - W_{k,\zeta_m}}{d_k} = \sum_{i=m}^t j_{k,i} \frac{Z_{i,\zeta_m}}{d_i} = \frac{j_{k,m}}{d_m},$$

with the final equality following because  $Z_{i,\zeta_m} = 0$  for all  $i \in [m+1, t]$ . Thus

$$Z_{k,\zeta_m} - W_{k,\zeta_m} = j_{k,m} \frac{d_k}{d_m}. \quad (5.13)$$

Since both  $Z_{k,\zeta_m}$  and  $W_{k,\zeta_m}$  satisfy condition (vi), that is, they are both in the interval  $[0, d_k/d_m)$ , it follows that (5.13) can be satisfied only if  $j_{k,m} = 0$ .

It follows from (5.13) that, contrary to the hypothesis,  $Z_{k,\zeta_m} = W_{k,\zeta_m}$  for all  $k$ , and so column  $\zeta_m$  of  $Z$  and  $W$  also coincide. Thus the hypothesis that columns  $\zeta_1, \zeta_2, \dots, \zeta_{m-1}$  of  $Z$  and  $W$  coincide leads to the same being true of column  $\zeta_m$  and to  $j_{k,m} = 0$  for  $k \in [1, m]$ .

An elementary inductive process leads to

$$j_{k,m} = 0 \quad \forall k, m \in [1, t].$$

This establishes that  $\mathbf{w}_k = \mathbf{z}_k$ ,  $k \in [1, t]$ , and so  $Z = W$  from which we conclude that  $Z$  is unique.  $\square$

## 6 Concluding Remarks

The principal result of this paper is the derivation of a unique canonical form for a fundamental class of lattice rules, namely, rules of prime-power order. Particularly encouraging is that this form is easy to recognize. Moreover, since the various proofs are constructive in nature, it is not difficult to construct an algorithm based on these proofs, which reduces any  $D - Z$  form for a prime-power rule into an ultratriangular form.

An interesting feature of this paper is that no use has been made of group theory, as in [SL89]; of lattice theory (in the form of generator matrices), as in [LSø93] or [LK95]; or even of the order property of individual lattice points, as in [L93]. The entire theory is developed independently, starting from an elementary definition (1.1) and employing only elementary transformations of integer matrices  $D$  and  $Z$ . The bibliography is composed of related papers. None are needed to understand this paper.

Naturally, both authors are in favor of exploiting all advanced theory when applicable. But it appeared in our development that elementary matrix theory is generally

sufficient. The single point when a minor improvement might have resulted is in the definition of the invariants. These essentially group-theoretic concepts turn out, in the case of prime-power rules, to have a concrete interpretation in terms of the orders of the set of projections of the rules. This property is of interest in its own right, but we would have preferred some more elegant property to define the term invariant.

The principal result (the unique canonical form) of this paper is confined to prime-power rules. In a recent paper [JS94] it is noted that any lattice rule may be expressed as a direct sum of prime-power rules. Our hope is that the present work will pave the way for results of wider generality, perhaps by exploitation of that direct sum.

## References

- [H62] E. Hlawka, *Zur angenäherten Berechnung mehrfacher Integrale*, Monatsh. Math. **66** (1962), 140–151.
- [HW81] L. K. Hua and Y. Wang, *Applications of number theory to numerical analysis*, Springer-Verlag, Berlin, 1981.
- [JS94] S. Joe and I. H. Sloan, *The direct sum of lattice rules*, Department of Mathematics and Statistics Research Report No. 30, 1994, The University of Waikato, Hamilton.
- [K59] N. M. Korobov, *The approximate computation of multiple integrals*, Dokl. Akad. Nauk SSSR **124** (1959), 1207–1210 (Russian).
- [L93] J. N. Lyness, *The canonical forms of a lattice rule*, in Numerical integration IV, ISNM 112 (H. Brass and G. Hämmerlin, eds.), Birkhäuser, Basel, 1993, pp. 225–240.
- [LK95] J. N. Lyness and P. Keast, *Application of the Smith normal form to the structure of lattice rules*, SIAM J. Matrix Anal. Appl. **16** (1995), 218–231.
- [LSø93] J.N. Lyness and T. Sørenvik, *Lattice rules by component scaling*, Math. Comput. **61** (1993), 799–820.
- [N73] H. Niederreiter, *Zur quantitativen Theorie der Gleichverteilung*, Monatsh. Math. **77** (1973), 55–62.
- [N78] H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), 957–1041.
- [N88] H. Niederreiter, *Quasi-Monte Carlo methods for multidimensional numerical integration*, in Numerical integration III, ISNM 85, (H. Brass and G. Hämmerlin, eds.), Birkhäuser, Basel, 1988, pp. 157–171.
- [SJ94] I. H. Sloan and S. Joe, *Lattice methods for multiple integration*, Clarendon Press, Oxford, 1994.



- [SL89] I. H. Sloan and J. N. Lyness, *The representation of lattice quadrature rules as multiple sums*, Math. Comput. **52** (1989), 81–94.
- [SL90] I. H. Sloan and J. N. Lyness, *Lattice rules: Projection regularity and unique representations*, Math. Comput. **54** (1990), 649–660.

Dr. J. N. Lyness  
Mathematics and Computer Science Division  
Argonne National Laboratory  
9700 South Cass Avenue  
Argonne, IL 60439  
U.S.A.  
lyness@mcs.anl.gov

Dr. S. Joe  
Department of Mathematics and Statistics  
The University of Waikato  
Private Bag 3105  
Hamilton  
New Zealand  
stephenj@hoiho.math.waikato.ac.nz